How can I identify a phishing attack?

To spot phishing emails, look out for the following:

- **Unexpected messages making unexpected requests**
  - Does this email or direct message come from an unfamiliar sender who claims to know you, or a friend who you have not spoken to in a long time? Does the list of recipients contain people you don’t know or talk to? This is particularly true if the message asks for money or personal information.

- **An offer that’s “too good to be true”**
  - It probably is, especially if important information like an employer’s address or a product’s shipping information is nowhere to be found.

- **Phishy Links and Email Addresses**
  - Hyperlinks and sender emails appear to correspond to known domains and people, but something, sometimes a single letter, has been changed. This may require close examination; look for misspellings, dashes, or other deviations from what seems to be a legitimate domain.

- **An email requests your password, your credit card number, or other sensitive information**
  - Email is never secure for sharing this information, and most trusted services should already have it. On sites which ask you to provide personal information, like your credit card, look for “https” in the address bar to ensure the site is secure.

- **An urgent tone**
  - If the sender says you must act now, uses fancy jargon or other intimidating language, ask yourself why.

- **Something “off”**
  - Phishing emails often have an impersonal, awkward, unprofessional, or out-of-character tone. Many, but not all, phishing emails contain conspicuous typos, bizarre capitalization, or numbers used in place of letters.

- **A prompt to open an attachment or follow a link**
  - Critically examine any email with an attachment, especially an unexpected one. If the link prompts you to “Sign In,” to an account, be extra suspicious. Do not “enable Macros” or allow similar permissions for attachments you do not trust.

- **The timezone/send time of the message is unusual**
  - For example, why would a member of the university community be sending a message with a time zone that is appropriate for eastern Europe? Is it suspicious for a UMBC community member to send an email message at 3am?

- **Valid name, but strange domain in email address.**
  - For example, UMBCPayroll@gmail.com, Freeman.Hrabowski@yahoo.com, or financialaid@umbc

- **Request for a cell phone number**
  - In many recent phishing messages, the hacker requests that you send them your cell phone number so that they can ask you a question. Why would a legitimate person needing assistance not just ask you the question in the email message rather than asking for your phone number?